

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
FACEBOOK USER 1260290777 THAT IS
STORED AT PREMISES CONTROLLED BY
FACEBOOK INC.

Case No. 17-570m

Filed Under Seal

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Thomas N. Carter, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain Facebook user ID that is stored at premises owned, maintained, controlled, or operated by Facebook Inc. ("Facebook"), a social networking company headquartered in Menlo Park, California. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Facebook to disclose to the government records and other information in its possession, pertaining to the subscriber or customer associated with the user ID. The account to be searched is under the name **CHRIS WOODS**, and has the associated **Facebook ID 1260290777** (hereinafter the "Target Account"). This account and the information to be searched is further described in the following paragraphs and in Attachment A.

2. I am a Special Agent with the Federal Bureau of Investigation, and have been for approximately 26 years. As part of my duties, I investigate violations of federal law, including the online exploitation of children, including violations pertaining to the illegal possession, receipt, transmission, and production of material depicting the sexual exploitation of minors, as

well as violations involving the coercion and enticement of minors to engage in illegal sexual activities. I have gained expertise in the conduct of such investigations through training in the area of child pornography and child exploitation investigations in seminars, classes, and everyday work related to conducting these types of investigations and have had the opportunity to observe and review numerous examples of child pornography in a variety of media, including computer media. I have obtained FBI Basic and Advanced Crimes Against Children Training. I have participated in the execution of numerous federal and state search warrants which have involved child sexual exploitation and/or child pornography offenses. I also work as a member of the Pittsburgh FBI Internet Crimes Against Children Task Force. By virtue of my FBI employment, I perform and have performed a variety of investigative tasks, including the execution of federal search warrants and seizures, and the identification and collection of computer-related evidence. I have personally participated in the execution of numerous federal search warrants involving the search and seizure of computer equipment in cases involving violations of Section 2252(a), 2250 and 2422(b), which involve the sexual exploitation of children.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended merely to show that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. As more fully set forth herein, your affiant submits that there is probable cause to believe that Christopher Robert WOODS violated Title 18, United States Code, Section 2252(a)(2) and (a)(4) by possessing, receiving and distributing child pornography. There is further cause to believe that WOODS violated or attempted to violate

Title 18, United States Code, Section 2422(b) by coercing and enticing a Minor to Engage in Unlawful Sexual Activity.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. §§ 2252(a) and 2422(b) have been committed by Christopher WOODS and that evidence of criminal offenses may be found in the Target Account. Moreover, based upon the same, there is probable cause to believe that the Target Account contains evidence and/or instrumentalities of these crimes, as further described in Attachment B.

PROBABLE CAUSE

5. From January 3-7, 2015, Jennifer Lynne Woods discovered emails and images on a computer in her home used exclusively by her husband that were sexually explicit and appeared to depict children engaged in sexually explicit conduct. Ms. Woods reported that the content on the computer included communications in which her husband discussed buying, selling and trading images of children who appeared to be under 18 years of age. Ms. Woods saved some of this content onto a gray Lexar 2GB thumb drive.¹ As of January 7, 2015, Ms. Woods and Christopher WOODS were living together, but Ms. Woods had initiated divorce proceedings. Ms. Woods and Christopher WOODS had two children, who also lived in the home with them: a son with a date of birth in 1998 and a daughter whose date of birth was in 1999.

6. Ms. Woods initially went to the Butler County District Attorney's Office and eventually the Evans City Seven Fields Regional Police Department to report her observations.

¹ This thumb drive has been marked and maintained by law enforcement, Evans City Police and the Pennsylvania State Police, as evidence tag number E0000173.

She provided a written statement in which she described finding two email accounts with “over 40,000 emails spanning 8 years.” Ms. Woods saw nude photos of girls that appeared to be prepubescent and some sexually explicit communications between her husband and girls claiming to be 13, 15 and “younger.” Some of these communications were perceived to be via Facebook instant messenger. According to Ms. Woods, in the communications, her husband also shared non-sexual pictures of Ms. Woods and their teenaged daughter, that had been posted on Facebook, but engaged in sexual chat about the two of them with others. Also in the communications, Christopher WOODS admitted to masturbating into his daughter’s underwear and expressed a desire to masturbate and ejaculate onto her breasts. One of the email accounts that Christopher WOODS used to engage in some communications was bigmaninpa@gmail.com.

7. On January 8, 2015, Evans City Police briefly accessed the thumb drive provided by Jennifer Woods and applied for and obtained a local search warrant for the residence of Christopher WOODS at 202 North Jackson Street, Evans City, PA, 16033. The search warrant was executed on the same date.

8. On April 27, 2017, this affiant met with Patrolman Scott M. Longdon of the Evans City Seven Fields Regional Police at the Butler County District Attorney’s Office. Ptlmn. Longdon affirmed the circumstances that preceded the execution of the search warrant at WOODS’ home in 2015. He also verified that the electronic devices that were seized in this investigation had been maintained in the custody of law enforcement, Evans City Seven Fields Regional Police and the Pennsylvania State Police, continuously since their seizure on January 8, 2015.

9. On May 3, 2017, this affiant interviewed Jennifer Woods at FBI Headquarters in Pittsburgh regarding her observations in 2015. Ms. Woods verified the information that she had provided to law enforcement previously. Ms. Woods and Christopher WOODS are now divorced.

10. On May 10, 2017, the Evans City Police tendered custody of computers and storage media obtained in the course of the investigation of Christopher WOODS to FBI to allow for federal investigation and further forensic analysis. The evidence is presently maintained at FBI Headquarters at 3311 East Carson Street in Pittsburgh, Pennsylvania. On May 10-12, 2017, your affiant reviewed the gray LEXAR thumb-drive originally obtained by the Evans City Police from Jennifer Woods.²

11. My review of the content of this thumb-drive revealed an email conversation between "Cobra Dragon" using email of: Alittlegirlie@yahoo.com and Bigmaninpa@gmail. Bigmaninpa@gmail.com was the email that was being utilized by Christopher WOODS in January 2015. (As of May 2017, a cursory review of internet social media and dating sites indicates that WOODS is continuing to use the handle "bigmaninpa" based upon photographs and consistent biographical data.) During the observed email exchange, it appears "Cobra Dragon"/Alittlegirlie@yahoo.com forwarded an email from "guycyrus@yahoo.com" which contained 5 images of young girls approximately 10-12 years old. Four of the images depict the young girls in swimwear and or underwear. One image depicts a pre-pubescent girl who appears approximately 10-12 years old: she is nude, positioned on all fours and her genitals are graphically exposed from the rear.

² As described in paragraphs 10 and 11, the Lexar thumb-drive was voluntarily provided by Ms. Woods to law enforcement on January 8, 2015.

12. The corresponding email discussion focuses upon the sexually explicit image of the nude female child. As "Bignnaninpa@gmail.com," WOODS, comments, "They last one is a nice view. Does tgat look like you. Are you as young and tiny as the cutie in the bikini?" Cobra Dragon/Alittlegirlie@yahoo.com replies, "lol im a little older than that but not much."

13. On May 17, 2017, in the course of my investigation, Jennifer Woods recalled the nature of the content that she saved to the Lexar thumb-drive and ultimately provided to the Evans City Police. Ms. Woods can still vividly recall the image of a young girl 10-12 years old, nude on all fours exposing her vagina and anus. She described it as an image that she cannot get out of her mind.

14. Ms. Woods also advised that she still had access to a Facebook page that she and Christopher WOODS used to share during their marriage. The account was originally set up as "ChrisnJyn" to signify both Christopher and Jennifer WOODS. In 2015, at or about the time that Ms. Woods discovered the sexually explicit chats and images on WOODS' computer, she had also observed sexually explicit messages between Christopher WOODS and others on the Facebook account to which they both had access. She detailed how WOODS would "share" images from Facebook of her, their teenaged daughter and their teenaged daughter's friends which were not sexual in nature. In conjunction with sharing these Facebook images, WOODS would engage in sexually explicit messaging with others about their daughter and their daughter's friends. He referred to having collected underwear from Jennifer Woods, their daughter and their daughter's friends and talked about providing it to others. WOODS made other statements indicative of a sexual interest in their daughter. Jennifer Woods informed me that she had accessed the Facebook page as recently as November 2016 and observed that some of the historical sexual messages were still present on the Facebook account. Following their

divorce and separation, Christopher WOODS modified the Facebook page to reflect that it is his personal account and not a joint account. According to Jennifer Woods, however, the account password remained the same and she was able to view the account as recently as May 2017.³

15. Records indicate that Christopher WOODS presently resides in Cranberry Township, Pennsylvania. Records further indicate a mailing address of P.O. Box 1562, Creekview Circle, Apt. 1401, Cranberry Township, PA, 16066.

16. Based on my knowledge, training, and experience, I know that electronic devices can store information for extended periods of time to include months and years. Similarly, content that has been viewed via the internet is typically stored for some period of time on the device. This information can sometimes be recovered with forensic tools. Also based upon my knowledge, training and experience, I know that the mere passage of time should not degrade electronic evidence that has been retained in police or law enforcement custody or that has been preserved by Facebook or other social media platforms.

17. Your affiant knows that Christopher WOODS has a Facebook account with Facebook user name **Chris WOODS** with associated **Facebook ID 1260290777**. Having interviewed Jennifer Woods in conjunction with the criminal investigation of WOODS, your affiant also knows that WOODS communicates via Facebook and Facebook Messenger (private message).

18. Considering all of the foregoing, probable cause exists that evidence of WOODS sexual interest in children and sexual exploitation of children may be found in the Target Account.

³ As of the date of this affidavit, Jennifer Woods reports that she could not access the Facebook account and believes that Christopher WOODS very recently changed the access password.

19. On May 24, 2017, your affiant sent a preservation request to Facebook for Christopher WOOD's account. As of today's date, Christopher WOODS' Facebook page was still active.

20. Facebook owns and operates a free-access social networking website of the same name that can be accessed at <http://www.facebook.com>. Facebook allows its users to establish accounts with Facebook, and users can then use their accounts to share written news, photographs, videos, and other information with other Facebook users, and sometimes with the general public.

21. Facebook asks users to provide basic contact and personal identifying information to Facebook, either during the registration process or thereafter. This information may include the user's full name, birth date, gender, contact e-mail addresses, Facebook passwords, Facebook security questions and answers (for password retrieval), physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers. Facebook also assigns a user identification number to each account.

22. Facebook users may join one or more groups or networks to connect and interact with other users who are members of the same group or network. Facebook assigns a group identification number to each group. A Facebook user can also connect directly with individual Facebook users by sending each user a "Friend Request." If the recipient of a "Friend Request" accepts the request, then the two users will become "Friends" for purposes of Facebook and can exchange communications or view information about each other. Each Facebook user's account includes a list of that user's "Friends" and a "News Feed," which highlights information about the user's "Friends," such as profile changes, upcoming events, and birthdays.

23. Facebook users can select different levels of privacy for the communications and information associated with their Facebook accounts. By adjusting these privacy settings, a Facebook user can make information available only to himself or herself, to particular Facebook users, or to anyone with access to the Internet, including people who are not Facebook users. A Facebook user can also create “lists” of Facebook friends to facilitate the application of these privacy settings. Facebook accounts also include other account settings that users can adjust to control, for example, the types of notifications they receive from Facebook.

24. Facebook users can create profiles that include photographs, lists of personal interests, and other information. Facebook users can also post “status” updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. Facebook users can also post information about upcoming “events,” such as social occasions, by listing the event’s time, location, host, and guest list. In addition, Facebook users can “check in” to particular locations or add their geographic locations to their Facebook posts, thereby revealing their geographic locations at particular dates and times. A particular user’s profile page also includes a “Wall,” which is a space where the user and his or her “Friends” can post messages, attachments, and links that will typically be visible to anyone who can view the user’s profile.

25. Facebook allows users to upload photos and videos, which may include any metadata such as location that the user transmitted when s/he uploaded the photo or video. It also provides users the ability to “tag” (i.e., label) other Facebook users in a photo or video. When a user is tagged in a photo or video, he or she receives a notification of the tag and a link to see the photo or video. For Facebook’s purposes, the photos and videos associated with a

user's account will include all photos and videos uploaded by that user that have not been deleted, as well as all photos and videos uploaded by any user that have that user tagged in them.

26. Facebook users can exchange private messages on Facebook with other users. These messages, which are similar to e-mail messages, are sent to the recipient's "Inbox" on Facebook, which also stores copies of messages sent by the recipient, as well as other information. Facebook users can also post comments on the Facebook profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile. In addition, Facebook has a Chat feature that allows users to send and receive instant messages through Facebook. These chat communications are stored in the chat history for the account. Facebook also has a Video Calling feature, and although Facebook does not record the calls themselves, it does keep records of the date of each call.

27. If a Facebook user does not want to interact with another user on Facebook, the first user can "block" the second user from seeing his or her account.

28. Facebook has a "like" feature that allows users to give positive feedback or connect to particular pages. Facebook users can "like" Facebook posts or updates, as well as webpages or content on third-party (*i.e.*, non-Facebook) websites. Facebook users can also become "fans" of particular Facebook pages.

29. Facebook has a search function that enables its users to search Facebook for keywords, usernames, or pages, among other things.

30. Each Facebook account has an activity log, which is a list of the user's posts and other Facebook activities from the inception of the account to the present. The activity log includes stories and photos that the user has been tagged in, as well as connections made through

the account, such as “liking” a Facebook page or adding someone as a friend. The activity log is visible to the user but cannot be viewed by people who visit the user’s Facebook page.

31. Facebook Notes is a blogging feature available to Facebook users, and it enables users to write and post notes or personal web logs (“blogs”), or to import their blogs from other services, such as Xanga, LiveJournal, and Blogger.

32. The Facebook Gifts feature allows users to send virtual “gifts” to their friends that appear as icons on the recipient’s profile page. Gifts cost money to purchase, and a personalized message can be attached to each gift. Facebook users can also send each other “pokes,” which are free and simply result in a notification to the recipient that he or she has been “poked” by the sender.

33. Facebook also has a Marketplace feature, which allows users to post free classified ads. Users can post items for sale, housing, jobs, and other items on the Marketplace.

34. In addition to the applications described above, Facebook also provides its users with access to thousands of other applications (“apps”) on the Facebook platform. When a Facebook user accesses or uses one of these applications, an update about that the user’s access or use of that application may appear on the user’s profile page.

35. Facebook uses the term “Neoprint” to describe an expanded view of a given user profile. The “Neoprint” for a given user can include the following information from the user’s profile: profile contact information; News Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends’ Facebook user identification numbers; groups and networks of which the user is a member, including the groups’ Facebook group identification numbers; future and past event postings;

rejected “Friend” requests; comments; gifts; pokes; tags; and information about the user’s access and use of Facebook applications.

36. Facebook also retains Internet Protocol (“IP”) logs for a given user ID or IP address. These logs may contain information about the actions taken by the user ID or IP address on Facebook, including information about the type of action, the date and time of the action, and the user ID and IP address associated with the action. For example, if a user views a Facebook profile, that user’s IP log would reflect the fact that the user viewed the profile, and would show when and from what IP address the user did so.

37. Social networking providers like Facebook typically retain additional information about their users’ accounts, such as information about the length of service (including start date), the types of service utilized, and the means and source of any payments associated with the service (including any credit card or bank account number). In some cases, Facebook users may communicate directly with Facebook about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Facebook typically retain records about such communications, including records of contacts between the user and the provider’s support services, as well as records of any actions taken by the provider or user as a result of the communications.

38. As explained herein, information stored in connection with a Facebook account may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, a Facebook user’s “Neoprint,” IP log, stored electronic communications, and other data retained by Facebook, can indicate who has used or controlled the Facebook account. This “user

attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, profile contact information, private messaging logs, status updates, and tagged photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the Facebook account at a relevant time. Further, Facebook account activity can show how and when the account was accessed or used. For example, as described herein, Facebook logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Facebook access, use, and events relating to the crime under investigation. Additionally, Facebook builds geo-location into some of its services. Geo-location allows, for example, users to “tag” their location in posts and Facebook “friends” to locate each other. This geographic and timeline information may tend to either inculcate or exculpate the Facebook account owner. Last, Facebook account activity may provide relevant insight into the Facebook account owner’s state of mind as it relates to the offense under investigation. For example, information on the Facebook account may indicate the owner’s motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

39. Therefore, the computers of Facebook are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Facebook, such as account access information, transaction information, and other account information.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

40. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Facebook to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

41. Based on the forgoing, I request that the Court issue the proposed search warrant.

42. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that – has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i). Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

REQUEST FOR SEALING

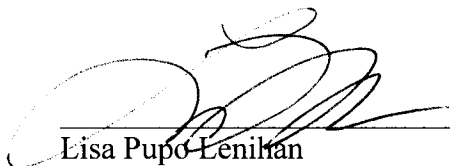
43. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

Respectfully submitted,



Thomas N. Carter
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on May 24, 2017



Lisa Pupo Lenihan
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the Facebook account held by **CHRISTOPHER WOODS** and associated with **Facebook ID 1260290777** that is stored at premises owned, maintained, controlled, or operated by Facebook Inc., a company headquartered in Menlo Park, California.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Facebook

To the extent that the information described in Attachment A is within the possession, custody, or control of Facebook Inc. ("Facebook"), including any messages, records, files, logs, or information that have been deleted but are still available to Facebook, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Facebook is required to disclose the following information to the government for each user ID listed in Attachment A:

- (a) All contact and personal identifying information, including full name, user identification number, birth date, gender, contact e-mail addresses, Facebook passwords, Facebook security questions and answers, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers.
- (b) All activity logs for the account and all other documents showing the user's posts and other Facebook activities;
- (c) All photos and videos uploaded by that user ID and all photos and videos uploaded by any user that have that user tagged in them;
- (d) All profile information; News Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments;

gifts; pokes; tags; and information about the user's access and use of Facebook applications;

- (e) All other records of communications and messages made or received by the user, including all private messages, chat history, video calling history, and pending "Friend" requests;
- (f) All "check ins" and other location information;
- (g) All IP logs, including all records of the IP addresses that logged into the account;
- (h) All records of the account's usage of the "Like" feature, including all Facebook posts and all non-Facebook webpages and content that the user has "liked";
- (i) All information about the Facebook pages that the account is or was a "fan" of;
- (j) All past and present lists of friends created by the account;
- (k) All records of Facebook searches performed by the account;
- (l) All information about the user's access and use of Facebook Marketplace;
- (m) The types of service utilized by the user;
- (n) The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);
- (o) All privacy settings and other account settings, including privacy settings for individual Facebook posts and activities, and all records showing which Facebook users have been blocked by the account;
- (p) All records pertaining to communications between Facebook and any person regarding the user or the user's Facebook account, including contacts with support services and records of actions taken.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. § 2252(a) and 2242(b) involving Christopher WOODS since January, 2015 including, for each user ID identified on Attachment A, information pertaining to the following matters:

- (a) Any and all communications to and from Christopher WOODS on referencing children, sexually explicit images of children or sexual acts involving children, underwear and/or sexual fantasies or objectification of children;
- (b) Evidence indicating how and when the Facebook account was accessed or used, to determine the chronological and geographic context of account access, use, and events relating to the crime under investigation and to the Facebook account owner;
- (c) Evidence indicating the Facebook account owner's state of mind as it relates to the crime under investigation;
- (d) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).
- (e) The identity of the person(s) who communicated with the Target Account about matters relating to the crimes under investigation;
- (f) Any other evidence relevant to the possible violations of 18 U.S.C. § 1512 being investigated in this matter.

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC BUSINESS
RECORDS PURSUANT TO FEDERAL RULE OF EVIDENCE 902(11)**

I, _____, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by Facebook, and my official title is _____. I am a custodian of records for Facebook. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Facebook, and that I am the custodian of the attached records consisting of _____ (pages/CDs/kilobytes). I further state that:

- a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;
- b. such records were kept in the ordinary course of a regularly conducted business activity of Facebook; and
- c. such records were made by Facebook as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

Date

Signature